FALNOA

AGENTES DE IA SOB CONTROLO

O que o DORA e o Regulamento da Inteligência Artificial pedem, em linguagem simples, e uma lista de verificação de 12 pontos.

BANCA E SEGUROS NA UNIÃO EUROPEIA

GUIA PRÁTICO · NOVEMBRO DE 2026

EM UM MINUTO

QUATRO IDEIAS

1

Os agentes de IA já não se limitam a responder.

Executam passos em processos reais: alteram registos, enviam mensagens, iniciam pagamentos.

2

O DORA aplica-se desde 17 de janeiro de 2025.

Não fala de agentes. Cobre os sistemas onde eles correm e os fornecedores que os entregam.

3

O Regulamento da IA adiou o risco elevado para 2 de dezembro de 2027.

As obrigações são as mesmas. Há mais tempo para as cumprir bem.

4

Controlo é conseguir responder a três perguntas.

Quem deixou o agente fazer isto, quem aprovou, e onde está a prova.

O PROBLEMA

DE RESPONDER A AGIR

Um assistente que responde mal dá uma má resposta. Um agente que age mal faz uma má transferência. O risco muda de natureza quando o software passa a ter mãos.

A OWASP chama a este risco «excesso de agência» e aponta três causas:

FUNÇÕES A MAIS

O agente tem acesso a ferramentas de que não precisa para a tarefa.

PERMISSÕES A MAIS

As ferramentas deixam-no fazer mais do que devia nos outros sistemas.

AUTONOMIA A MAIS

Ações com impacto avançam sem que uma pessoa as confirme.

QUEM O DEIXOU FAZER ISTO?
QUEM APROVOU?
ONDE FICOU REGISTADO?

Fonte: OWASP Top 10 for LLM Applications 2025, LLM06:2025 Excessive Agency.

O CALENDÁRIO

O QUE JÁ SE APLICA

17 JAN 2025

DORA

O regulamento aplica-se a bancos, seguradoras e outras entidades financeiras.

DORA ART. 64.º

2 FEV 2025

Regulamento da IA: práticas proibidas

As primeiras proibições entram em aplicação.

REG. IA ART. 113.º

2 AGO 2026

Regulamento da IA: transparência

Quem fala com uma IA tem de ser informado disso.

REG. IA ART. 50.º

HOJE: NOVEMBRO DE 2026

2 DEZ 2027

Risco elevado: usos do Anexo III

Crédito a particulares, seguros de vida e de saúde, recrutamento. Antes era 2 de agosto de 2026.

REG. (UE) 2026/1744

2 AGO 2028

Risco elevado: produtos regulados

Sistemas de IA incorporados em produtos do Anexo I.

REG. (UE) 2026/1744

> O adiamento veio com o Regulamento (UE) 2026/1744, publicado a 24 de julho de 2026 e em vigor desde 27 de julho de 2026.

Fontes: Regulamento (UE) 2022/2554; Regulamento (UE) 2024/1689, alterado pelo Regulamento (UE) 2026/1744; Comissão Europeia, «AI Act».

DORA EM LINGUAGEM SIMPLES

CINCO COISAS QUE O DORA PEDE

A ADMINISTRAÇÃO RESPONDE

ART. 5.º

O órgão de administração tem a responsabilidade final pela gestão do risco de TIC. Não se delega num fornecedor nem numa equipa técnica.

SAIBA O QUE TEM

ART. 8.º

Identificar e documentar as funções de negócio suportadas por TIC e os ativos de que dependem.

CONHEÇA OS FORNECEDORES

ART. 28.º

Manter um registo de informações de todos os contratos de serviços de TIC. Para funções críticas ou importantes, ter uma estratégia de saída.

TESTE

ART. 24.º

Ter um programa de testes. Os sistemas que suportam funções críticas ou importantes são testados pelo menos uma vez por ano.

COMUNIQUE OS INCIDENTES GRAVES

ARTS. 17.º E 19.º

Ter um processo para detetar, gerir e registar incidentes. Os graves seguem para a autoridade: notificação inicial, relatório intercalar, relatório final.

> **E os agentes?** O DORA não os menciona. Na nossa leitura, um agente que executa passos num processo crítico faz parte desse sistema. Se vem de um fornecedor, esse contrato pertence ao registo.

Fonte: Regulamento (UE) 2022/2554. Modelos do registo de informações: Regulamento de Execução (UE) 2024/2956.

REGULAMENTO DA IA EM LINGUAGEM SIMPLES

QUANDO É RISCO ELEVADO, E O QUE MUDA

É RISCO ELEVADO QUANDO

ANEXO III

O sistema avalia a solvabilidade ou a pontuação de crédito de pessoas (exceto deteção de fraude), avalia risco e preços em seguros de vida e de saúde, ou é usado para recrutar e decidir sobre trabalhadores.

PESSOAS COM AUTORIDADE

ARTS. 14.º E 26.º

A supervisão humana é entregue a pessoas com competência, formação e autoridade. Têm de poder ignorar ou reverter um resultado e parar o sistema.

REGISTOS GUARDADOS

ARTS. 12.º E 26.º

O sistema regista eventos automaticamente. Quem o usa guarda esses registos pelo menos seis meses. As instituições financeiras guardam-nos com a documentação que a lei financeira já exige.

AVALIAR O IMPACTO

ART. 27.º

Antes de usar um sistema de crédito ou de seguros de vida e saúde, avaliar o impacto nos direitos fundamentais.

JÁ SE APLICA

ART. 50.º

Uma pessoa que interage com uma IA tem de ser informada disso, a menos que seja óbvio.

> **Um agente é um «sistema de IA»?** A definição cobre sistemas que funcionam «com níveis de autonomia variáveis» (art. 3.º). O RGPD continua a aplicar-se às decisões exclusivamente automatizadas (art. 22.º).

Fontes: Regulamento (UE) 2024/1689, alterado pelo Regulamento (UE) 2026/1744; Regulamento (UE) 2016/679.

ADIADO NÃO É DISPENSADO

O prazo do risco elevado mudou. As obrigações não mudaram. E o DORA já se aplica hoje a qualquer agente que toque num processo crítico.

LISTA DE VERIFICAÇÃO

12 PONTOS, SIM OU NÃO

SABER O QUE EXISTE

- [ ] 01 **Cada agente está num inventário.**
  Com finalidade, modelo e dados que usa.
  DORA 8.º

- [ ] 02 **Cada agente tem um dono.**
  Uma pessoa com nome, não uma equipa.
  DORA 5.º
  REG. IA 26.º

- [ ] 03 **Os fornecedores estão no registo.**
  Modelos e agentes de terceiros, com plano de saída.
  DORA 28.º

CONTROLAR ANTES DA AÇÃO

- [ ] 04 **Os limites estão escritos.**
  O que cada agente faz sozinho e o que espera por uma pessoa.
  REG. IA 14.º
  OWASP LLM06

- [ ] 05 **As ações com impacto esperam por aprovação.**
  Com motivo escrito. Duas pessoas nas maiores.
  REG. IA 14.º
  BOA PRÁTICA

- [ ] 06 **Consegue parar todos os agentes de uma vez.**
  E já experimentou.
  REG. IA 14.º

LISTA DE VERIFICAÇÃO

12 PONTOS, CONTINUAÇÃO

PROVAR DEPOIS DA AÇÃO

- [ ] 07 **Cada ação e cada aprovação fica registada.**
  Quem, o quê, quando e porquê.
  REG. IA 12.º, 26.º

- [ ] 08 **Consegue mostrar que o registo não foi alterado.**
  Uma cópia adulterada é detetada.
  BOA PRÁTICA

- [ ] 09 **Um auditor chega à prova sem um projeto à parte.**
  Acesso só de leitura, limitado no tempo.
  BOA PRÁTICA

TESTAR E RESPONDER

- [ ] 10 **Nenhuma alteração vai para produção sem testes.**
  As mesmas perguntas, repetidas a cada mudança.
  DORA 24.º
  REG. IA 15.º

- [ ] 11 **Tenta-se enganar o agente, de propósito.**
  Injeção de instruções, fuga de dados.
  DORA 24.º
  OWASP

- [ ] 12 **Uma falha de um agente entra no processo de incidentes.**
  Com os prazos de reporte definidos.
  DORA 17.º, 19.º

> Por onde começar: pelos pontos 1, 5 e 7. Sem inventário, aprovação e registo, os outros não se sustentam.

COMO RESPONDE A BLUE FALNOA

OS MESMOS QUATRO VERBOS, NUMA APLICAÇÃO

A Blue Falnoa é a aplicação onde as pessoas supervisionam os agentes de IA da empresa. Liga-se aos agentes que já existem.

SABER

- **Registo de sistemas de IA**: cada agente com dono, finalidade, modelo, dados e classe de risco.
- **Registo de fornecedores de TIC e de IA**: criticidade, localização, fim de contrato, plano de saída. Exporta para folha de cálculo.

CONTROLAR

- **Gateway de ações**: o agente pede antes de agir e espera pela decisão.
- **Regras por valor, risco, hora e tipo de ação**, com aprovação por duas pessoas e motivo escrito.
- **Paragem de emergência**: suspende todos os agentes de uma vez.

PROVAR

- **Registo de auditoria encadeado**: uma cópia alterada é detetada.
- **Selos assinados** que se verificam fora da aplicação, sem ligação à rede.
- **Portal do auditor**: conta só de leitura que termina sozinha.

TESTAR

- **Avaliações e portões de lançamento**: uma versão só é lançada acima de uma nota mínima.
- **Campanhas adversariais**: injeção, fuga do prompt, extração de segredos.
- **Registo de incidentes** com relógio de reporte e prazos editáveis.

Uma instância por cliente, na infraestrutura do cliente. Interface em português e inglês.

COM HONESTIDADE

O QUE A BLUE FALNOA NÃO É

✕ Não é uma certificação

A Falnoa não tem relatório SOC 2 nem certificado ISO 27001. Ainda não foi feito um teste de intrusão externo.

✕ Não é aconselhamento jurídico

A aplicação organiza controlo e prova. Se isso cumpre uma obrigação concreta, decide cada entidade com os seus juristas.

✕ Não controla quem não lhe pergunta

O gateway é um ponto de controlo para os agentes que o chamam. Ligar cada agente faz parte do trabalho.

✕ Não está provada em todo o lado

Publicamos o que foi verificado a sério, o que só tem testes automáticos e o que não foi feito.

> O livro de estado é público: falnoa.com/pt/trust/status-ledger

FONTES

ONDE CONFIRMAR

1 Regulamento (UE) 2022/2554, relativo à resiliência operacional digital do setor financeiro (DORA). Arts. 5.º, 8.º, 17.º, 19.º, 24.º, 28.º e 64.º.
https://eur-lex.europa.eu/eli/reg/2022/2554/oj

2 Regulamento de Execução (UE) 2024/2956, modelos normalizados para o registo de informações.
https://eur-lex.europa.eu/eli/reg_impl/2024/2956/oj

3 Regulamento (UE) 2024/1689, Regulamento da Inteligência Artificial. Arts. 3.º, 12.º, 14.º, 15.º, 26.º, 27.º, 50.º, 113.º e Anexo III.
https://eur-lex.europa.eu/eli/reg/2024/1689/oj

4 Regulamento (UE) 2026/1744, que altera o Regulamento (UE) 2024/1689 («Digital Omnibus» da IA).
https://eur-lex.europa.eu/eli/reg/2026/1744/oj

5 Comissão Europeia, «AI Act», calendário de aplicação. Consultado a 13 de novembro de 2026.
https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

6 Regulamento (UE) 2016/679 (RGPD), art. 22.º.
https://eur-lex.europa.eu/eli/reg/2016/679/oj

7 OWASP Top 10 for LLM Applications 2025, LLM06:2025 Excessive Agency.
https://genai.owasp.org/llmrisk/llm062025-excessive-agency/

Este guia resume textos legais em linguagem simples e não é aconselhamento jurídico. As referências a artigos servem para orientar a leitura. Confirme sempre na versão consolidada em vigor e com os seus juristas. As ligações entre o DORA e os agentes de IA são a leitura da Falnoa, não uma posição de qualquer autoridade. Nenhuma norma cita a Blue Falnoa e a Falnoa não detém certificações. Factos regulatórios verificados a 13 de novembro de 2026.

QUER VER ISTO A FUNCIONAR?

falnoa.com/pt/products/blue-falnoa
hello@falnoa.com

© 2026 Falnoa